REMARKS

Claims 1-3, 7-13, 16-19, 21, 22 and 25-27 were pending and presented for examination and in this application. Claims 1, 7-10, 16, 18, 19, 21, 25, and 27 are amended herein, and claims 26 and 27 are cancelled. New claims 28 and 29 have been added. In view of the Amendments and the Remarks that follow, Applicant respectfully requests that Examiner reconsider all outstanding rejections, and withdraw them.

Interview Summary

On June 16, 2010, Examiner Greene and Applicant's representative, Antonia Sequeira, had a telephone interview to discuss the section 103 rejection of the claims based on Moore and Yufik. Applicant presented arguments similar to those presented below. The Examiner suggested that the Applicant provide additional amendments regarding the first and second tokens, to further clarify the claim language. Applicant has amended the claims as suggested by the Examiner. The Examiner agreed that the claim amendments as presented above would likely overcome the Moore and Yufik references. Applicant thanks the Examiner for his time and consideration in this case.

Response to Rejection Under 35 USC 103(a)

The Examiner rejects claims 1, 9-10, 18-19, 21-22, 25 and 27 under 35 USC § 103(a) as allegedly being unpatentable over Moore et al. (U.S. Patent No. 7,000,015) in view of Yufik (U.S. Patent No. 5,794,224). This rejection is respectfully traversed.

Claim 1 as amended recites:

> A method for associating computer network detectors and network interfaces with network policies, said method comprising the steps of:
>
> analyzing one or more network interfaces associated with a client computer using a plurality of network detectors, the detectors outputting a set of a plurality of netspecs, each netspec comprising a first token that is a detector token having

a static value that identifies a specific detector that created the netspec and a second token that is a value that the specific detector uses to uniquely identify the analyzed network interface;

determining that a first detector outputted a first netspec for a particular analyzed network interface of the one or more network interfaces and that a second detector outputted a second netspec for the particular analyzed network interface;

determining that the first detector is more reliable in observing the particular analyzed network interface than is the second detector;

awarding a higher priority to the first netspec than to the second netspec in response to the first netspec being output by the first detector and the first detector being more reliable than the second detector;

associating the first netspec that was awarded the higher priority with a location that is linked to one or more network policies designated by a user to be implemented for the location; and

feeding the associated netspec/location pair to a network interface module to implement the one or more network policies designated for the location.

The combination of Moore and Yufik fails to teach various elements of the claims. First, Moore fails to teach "analyzing one or more network interfaces…each netspec comprising a *first token that is a detector token having a static value that identifies a specific detector that created the netspec* and a second token that is a value that the specific detector uses to uniquely identify the analyzed network interface." As recited in claim 1, a netspec comprises two tokens – a first token that is a detector token identifying the detector itself and a second token identifying the network interface analyzed by that detector. Moore does not teach at least the *first token*. The Examiner cites Moore's GUID as allegedly disclosing the first token or detector token. The GUID however is defined in Moore as "a globally unique identifier (GUID) … that *identifies the computer's physical network interface* through which the network is accessible." Moore, col. 14, 17-20 (emphasis added). The GUID is at best the second token that *identifies the network interface*. There is no disclosure of the GUID *being a detector token that identifying a specific detector*, as the claim recites, and so there is no teaching of a first token. Further, the Examiner argues that the network detectors are taught in Moore's NLRSP, and states that the NLRSP is "a set of services that combined form *the plurality of network detectors*." Office Action, page 2-3 (emphasis added). If the NLRSP services were the network detectors, as the Examiner alleges,

then the first token (detector token which identifies the detector) would have to be a token identifying one of the NLRSP services. Yet, Moore does not disclose any token or identifier for different services within the NLRSP. Thus, Moore fails to disclose at least the first token of the netspec, as claimed. Yufik also fails to disclose this element and the Examiner does not argue otherwise.

Second, Moore fails to teach "determining that a *first detector outputted a first netspec for a particular analyzed network interface* of the one or more network interfaces and that a *second detector outputted a second netspec for the particular analyzed network interface*." Moore fails to disclose two different network detectors that each output a netspec *for the same network interface*. Even if the NLRSP of Moore did include a "set of services that combined form the plurality of network detectors" as the Examiner alleged, Moore fails to disclose two different NLRSP services *analyzing the same network interface* and *each outputting a netspec for that interface*. Under the Examiner's interpretation of the NLRSP being a set of services that are the detectors and the GUID being a token, two NLRSP services would have to analyze the same interface and output a different GUID for the interface. However, Moore does not disclose this, and so fails to teach the claimed step. Yufik also does not disclose this element, and the Examiner does not argue otherwise.

Third, Yufik fails to teach "determining that the first detector is more reliable in observing the particular analyzed network interface than is the second detector." The Examiner relies on Yufik for this element. However, Yufik discloses a system of resource allocation, where network links between starting and terminal nodes are weighted based on the frequency and relative success of exercising the same network links in past allocation decisions. *See id.* Thus, reliability in the context of Yufik is limited to the success of the communicative capability of a network link. Id., col. 7, 63-67; col. 8, 1-5. In contrast, claim 1 discloses determining which of two network detector is more reliable *in observing the same network interface*, which is reliability in terms of the functional capability of the network detector. The Examiner also argued that "the nodes of Yufik are specifically weighted based on their reliability … thus, their relative weights will be utilized when determining (between two or more), which node to use,"

and argued that Moore teaches the concept of observing an interface. Office Action, page 16. Even if Moore's observing of an interface were combined with the Yufik's determination of network link communicative reliability, this still fails to teach determining that one detectors is more reliable than another in observing an interface. At most, this teaches using a detector to observe a network interface to determine how communicatively reliable it is, but not *determining how reliable a detector is in observing an interface*. Furthermore, Moore does not even disclose two network detectors observing *the same network interface*, and so the combination of Moore and Yufik does not teach determining that one detector is more reliable than another in observing a particular interface. Thus, the Moore and Yufik combination fails to teach the claimed element.

Fourth, Yufik fails to disclose "awarding a higher priority to the first netspec in response to the first netspec being output by the first detector and the first detector being more reliable than the second detector." The Examiner relies on Yufik for this element. As stated above, determining which of two network detectors is more reliable in observing a particular analyzed network interface is not disclosed by Moore and Yufik. In addition, awarding a higher priority to a netspec of a detector in response to the detector being more reliable in observing a particular network interface than another detector is in observing that particular interface is likewise not disclosed.

Claims 2-3, 6-8, 11-13, and 16-17 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Moore in view Yufik and further in view of Aaron (U.S. Publication No. 2004/0268150).

For at least the reasons stated above regarding why the combination of Moore and Yufik fails to disclose all of the elements of the independent claims, the combination also fails to disclose the elements of dependent claims 2-3, 6-8, 11-13, and 16-17. Aaron does not remedy the deficiencies in Moore and Yufik. Aaron discloses a system for providing network-based firewall policy configuration and facilitation. *See* Aaron, Abstract. A policy modification agent ("PMA") resides on a memory along with an operating system. *See* Aaron, [0028]. A user sends a notification to a firewall facilitation coordinator ("FFC") to modify the user's firewall policy

for a new application. The FFC receives the notification and authenticates the user. The FFC sends a request to the PMA seeking modification of the firewall policy as applied to the new application. *See* Aaron, [0044]. Upon receiving the request, the PMA initiates an "exercise period". During the exercise period the PMA observes packets associated with the new application. *See* Aaron, [0046]. The PMA then generates rules for filtering the packets based on whether questionable packets are observed during this exercise period. *See* Aaron, [0047]-[0050] and FIGS. 5A-5D. However, like Moore and Yufik, Aaron does not disclose outputting netspecs comprising a token identifying a detector which outputted the netspec and a token identifying an analyzed network interface, determining that two different detectors output a netspec for the same analyzed network interface, or determining that a first network detector is more reliable than a second network detector in observing that particular analyzed network interface, nor does the Examiner claim that it does.

Thus, Moore, Yufik and Aaron, either alone or in the combination suggested by the Examiner, do not teach or suggest every element of independent claims 1, 10, and 21, nor the claims depending therefrom. Accordingly, Applicant requests withdrawal of this rejection.

CONCLUSION

Withdrawal of the pending rejections and reconsideration of the claims are respectfully requested, and a notice of allowance is earnestly solicited. If the Examiner has any questions concerning this Response, the Examiner is invited to telephone Applicant's representative at (650) 335-7185.

Respectfully Submitted,
Peter Linhardt

Date: June 17, 2010 By: /Antonia L. Sequeira/

Antonia L. Sequeira, Esq.
Reg. No. 54,670
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel (650) 335-7185
Fax (650) 938-5200